Hinweise zur europäischen Datenschutzgrundverordnung (DSGVO) für Ingenieurinnen und Ingenieure

Bitte beachten Sie, dass folgende Hinweise nur als kurzer Leitfaden zu verstehen sind und eine fundierte ***rechtliche Beratung nicht ersetzen können****. Im Bedarfsfall sollten Sie Ihren Rechtsanwalt oder Datenschutzbeauftragten konsultieren.*

Die europäische Datenschutzgrundverordnung (DSGVO) gilt ab dem 25. Mai 2018, nachdem ein Zeitraum von 2 Jahren für die Umsetzung entsprechender Maßnahmen eingeräumt worden war. Zeitgleich gilt eine neue Fassung des Bundesdatenschutzgesetzes (BDSG). Doch nicht jeder konnte die Zeit nutzen, nötige Änderungen der bestehenden Strukturen durchzuführen. Mit der DSGVO werden Rechenschaftspflichten eingeführt, bei deren Verletzung empfindliche Strafen drohen. Um diese abzuwenden, bedarf es einer ausführlichen Dokumentation der Einhaltung der notwendigen Maßnahmen.
Hierfür möchten wir Ihnen einige Hinweise speziell für Ingenieurinnen und Ingenieure geben.

Was ist die DSGVO?

Die europäische DSGVO ist eine Verordnung, die unmittelbar in allen Mitgliedsstaaten der EU – also auch Deutschland – gilt. Unmittelbar heißt, dass die Regelungen ohne eine besondere Umsetzung Geltung entfalten. Ergänzende Bestimmungen finden sich im neuen BDSG.

Was regelt die DSGVO?

Die DSGVO erfasst personenbezogene Daten. Nach der gesetzlichen Definition des Art. 4 Nr. 1 DSGVO sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen.
Die Verarbeitung dieser Daten muss auf einer rechtlichen Grundlage beruhen, deren Einhaltung nachgewiesen werden muss.

Wen betrifft die DSGVO?

Die DSGVO betrifft alle, die personenbezogene Daten in der EU verarbeiten und damit auch alle Ingenieurbüros, die Daten von natürlichen Personen verarbeiten wie z.B. von Auftraggebern oder Bauherren. Es gibt keine generellen Ausnahmen für kleine oder mittlere Unternehmen.

Was ist zu tun?

Die unternehmensinternen Datenflüsse und die IT-Infrastruktur sind zu untersuchen. Alle, die noch keine interne Übersicht über die Datenflüsse aufgestellt haben, sollten dies tun. So kann ein Verarbeitungsverzeichnis entstehen, in dem die Datenverarbeitung festgehalten wird. Wer verarbeitet hier

wo welche Daten zu welchem Zweck – hier ist nicht nur das Sekretariat betroffen, das die Rechnungen schreibt. Vielmehr ist jede Ingenieurin / jeder Ingenieur datenverarbeitend tätig, wenn sie / er Korrespondenz mit einem Auftraggeber führt, da dieser namentlich erfasst wird.
Wenn die Datenströme lokalisiert worden sind, bedarf es einer Klärung, welche Art von Daten vorliegen. Handelt es sich um „personenbezogene Daten“[1] oder gar um „besondere personenbezogene Daten“[2]? Besteht ein hohes Risiko für die betroffenen Personen, bspw. finanzieller Verlust bei Bankdaten oder Identitätsdiebstahl bei sozialen Profilen, so muss eine Datenschutzfolgeabschätzung (DSFA) durchgeführt werden, bei der mögliche Risiken und Angriffsszenarien bewertet, geeignete Schutzmaßnahmen implementiert werden und ein Bericht verfasst wird.

Welche besonderen Pflichten bestehen?

Bei der Erfassung von personenbezogene Daten müssen durch die verantwortliche Stelle gegenüber dem Betroffen bestimmte Informationspflichten (Art. 13 DSGVO) erfüllt werden.
Der Betroffene ist darüber aufzuklären (i) wer die *Daten zu welchem Zweck wie lange* verarbeitet, (ii) dass er ein *Auskunftsrecht* besitzt, (iii) dass ihm ein Recht auf Berichtigung zusteht, (iv) dass ein *Recht auf Löschung* besteht, (v) dass ein *Recht auf Einschränkung der Bearbeitung besteht*, (vi) dass ein *Recht auf Widerspruch* und ein (vii) *Recht auf Datenübertragbarkeit* bestehen.
Es bietet sich an, einem Betroffenen zu Beginn des Auftrags ein Merkblatt auszuhändigen, das die Informationspflichten erfüllt und ein unterzeichnetes Exemplar in die Akte zu nehmen, damit die Dokumentation gewährleistet und der Nachweis gegenüber den Datenschutzbehörden erfüllt werden kann.

Muss ein Datenschutzbeauftragter bestellt werden?

Nach § 38 Abs. 1 ist ein Datenschutzbeauftragter (DSB) zu benennen, wenn *mindestens 10 Personen* ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Damit sind nur sehr kleine Ingenieurbüros von der Verpflichtung, einen DSB zu benennen, ausgenommen. Der Datenschutzbeauftragte muss fachlich geeignet und von der Geschäftsleitung unabhängig sein. Die Bestellung des Geschäftsführers als DSB ist damit nicht möglich.

[1]Nach Art. 4 DSGVO sind „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
[2] Nach Art. 9 DSGVO ist die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person untersagt.

Was passiert bei einem Verstoß?

Die datenschutzrechtliche Thematik nimmt an Wichtigkeit zu und durch die Einführung der DSGVO können und müssen die Aufsichtsbehörden aktiver werden, als es bislang der Fall war. Unterschiedliche Aufsichtsbehörden sind bereits tätig geworden und haben noch vor Geltung der DSGVO an bestimmte Berufsgruppen Fragebögen zur Einhaltung der DSGVO verschickt, so z.B. der Landesdatenschutzbeauftragte für Mecklenburg-Vorpommern an die Ärzteschaft.

Bei Verstößen gegen Anweisungen der Aufsichtsbehörde können Geldbußen bis zu 20.000.000,- € oder von bis zu 4% des gesamten weltweiten Umsatzes verhängt werden. Diese Zahlen machen deutlich, dass ein unbeschwerter Umgang mit personenbezogenen Daten in Zukunft nicht mehr möglich sein wird.

Checkliste – Das sollten Sie prüfen:

- Prüfung der vorliegenden Daten und Anfertigen einer Übersicht
- Prüfung zur Berechtigung für eine Datenverarbeitung
- Prüfung von Dritten (Dienstleister oder verbundene Unternehmen, die Datenzugriff haben) – bestehen hier konforme Vereinbarungen zur Datenverarbeitung im Auftrag?
- Prüfung – muss ein Datenschutzbeauftragter bestellt werden?
- Prüfung – gibt es ein Verarbeitungsverzeichnis?
- Prüfung – muss eine Datenschutzfolgeabschätzung (DSFA) durchgeführt werden?
- Prüfung der eigenen Website / Homepage hinsichtlich der Datenschutzerklärung

Autor: Dr. iur. Nadim Kashlan, LL.M., Rechtsanwalt und Fachanwalt für Informationstechnologierecht, Wiesbaden

Weitere Informationen im Internet

Auslegungshilfen zum Datenschutzrecht finden Sie auch auf der Internetseite des Hessischen Datenschutzbeauftragten:
https://www.datenschutz.hessen.de/neuesdatenschutzrecht.htm

Die Gesellschaft für Datenschutz und Datensicherheit fasst die Änderungen im Vortrag von Dr. Matthias Scholz zusammen:
https://www.gdd.de/eforen/hessen/veranstaltungen/erfa-kreis-hessen-sitzung-herbst-2016/die-datenschutz-grundverordnung-ist-da-was-aendert-sich-dr-matthias-scholz-1/view

Die Publikation des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (bitcom e. V.): „Was muss ich wissen zur EU-Datenschutz Grundverordnung?“
https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/160909-EU-DS-GVO-FAQ-03.pdf